

NAVAL WAR COLLEGE
Newport, RI

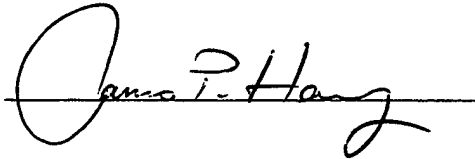
Circumstance and Technology:
The Effective Tasking and Use of Network-based Assets

J.P. Harvey
Major, United States Air Force

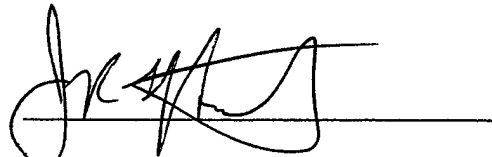
A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations Department.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College, the Department of the Navy, or the Department of the Air Force.

Signature: _____



8 February 2000



J. R. FitzSimonds
CAPT USN

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

DTIC QUALITY INSPECTED 4

20000621 135

A

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: 1C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): Technology and Circumstance: The Effective Tasking and Use of Network-based Assets (Unclassified)			
9. Personal Authors: Major James P. Harvey, USAF			
10. Type of Report: FINAL		11. Date of Report: 8 February 2000	
12. Page Count: 22 12A Paper Advisor (if any): CAPTAIN James R. FitzSimonds, USN			
13. Supplementary Notation: A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC, the Department of the Navy, or the Department of the Air Force.			
14. Ten key words that relate to your paper: network; platform; intelligence; distributed; reachback; technology; revolution in military affairs; culture			
15. Abstract: <p>Two forces are shaping today's environment, drawing attention to the need to move from a platform-based doctrine of warfighting to one that embraces network-based assets. These two forces are circumstance and technology. The Air Forces Deployable Ground Station Two is a modern, network-based asset and serves as a model throughout the paper. This organization's employment over the past five years illustrates not only the increased capabilities that network-based assets contribute to the operational commander, but also serves to demonstrate the tendency to limit these contributions. These limitations occur when network-based assets (albeit in their infancy) are employed through platform-based models.</p> <p>Joint and Service doctrine must build upon the conceptual template established in Joint Vision 2010 with the development of new doctrine that addresses the unique capabilities of network-based assets. This doctrine should encompass the relationship between networks and platforms so as to maximize the combat power afforded by each.</p> <p>Consideration is also given to reorganization as well as the possibility for development of new organizations in the future, designed to best employ network-based resources for the operational commander. If the military acknowledges these emerging capabilities, it is well on the way to establishing a credible doctrine to accompany its emerging network-based weapon systems.</p>			
16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-6461		20. Office Symbol: C	

Security Classification of This Page Unclassified

[T]he information revolution is not solely or mainly about technology; it is an organizational as well as technological revolution. Thus, the emphasis...is less on the advance of technology than on the challenges for organization—and on the interactions between technological and organizational changes that have implications for doctrine and strategy. ...[T]he information revolution favors and strengthens network forms of organization, while making life difficult for hierarchical forms. The rise of network forms of organization—particularly “all channel networks,” in which every node can communicate with every other node—is one of the single most important effects of the information revolution for all realms: political, economic, social, and military.... This will place the U.S. military (and police) forces under growing pressure to formulate new concepts for organization, doctrine, strategy, and tactics. ...[T]wo new models of conflict in particular are going to define the information-age conflict spectrum: what we term “cyberwar” and “netwar”. Both terms refer to comprehensive approaches to conflict based on the centrality of information—comprehensive in that they combine organizational, doctrinal, strategic, tactical, and technological innovations, for both offense and defense. ...The United States is the only country with the array of advanced technologies (e.g., for command and control, surveillance, stealth, etc.) as well as the organizational and doctrinal flexibility to make cyberwar an attractive and feasible option. But its potential adversaries, especially nonstate adversaries, may have the lead in regard to netwar. (Arquilla and Ronfeldt, *In Athena's Camp*)¹

INTRODUCTION: THE CIRCUMSTANCES AND TECHNOLOGY

Several significant changes have occurred since the end of the Gulf War, spanning a variety of areas, all touching in some way on the issue of U.S. national security. If there were two words that best capture these changes, they are *circumstance* and *technology*. Both have contributed to the contemporary disposition of the U.S. armed forces, the philosophy behind overseas basing, and the methods with which we project and employ combat power today, and plan to do so in the future. The combination of these two changes should only be viewed as an opportunity for a needed change.

This paper addresses one of the changes that may prove to deliver the broadest impact on future doctrine and strategy relative to the U.S. military operations of tomorrow: the migration from platform-based to network-based warfighting capabilities. This change—based on emerging technology (such as “high-bandwidth” satellite communications) and demonstrated in

its infancy courtesy of circumstance outside of the military's control (a political preference for less forward presence and more CONUS-based expeditionary operations, force protection concerns, budgetary constraints, force reductions, etc.)—is demonstrating new capabilities (“virtual augmentation” and support), and inviting some reasonable concerns as well. Perhaps the greatest concerns are due to traditional (platform-based) models of ownership and force employment, doubts about the reliability of virtual systems, control and responsiveness. These rapidly surfaced as demonstrations of network-based capabilities began replacing what was only academic banter in the past. During our tenure in the Balkans, the U.S. military has seen and truly employed some of the emerging network-based weapon systems and assets.

To facilitate the proper tasking and employment of emerging network-based assets, new joint doctrine must embrace the unique nature of these systems. This doctrine, leveraging off the Joint Vision 2010 foundation, will best serve as a vehicle to encourage the cultural change required within the Department of Defense (DoD); a change that will embrace new network-based along with traditional platform-based assets.

To gain maximum benefit from both current and emerging network-based capabilities, joint doctrine and the military culture must change to address new methods of tasking and employing these virtual weapon systems and assets. Given the current uniqueness of these network-based capabilities, they typically fall into the high demand/low density (HD/LD) category of assets, and are found predominantly in information and intelligence organizations. Currently the U.S. Air Force operates two Deployable Ground Stations (DGSs), intelligence assets currently fed by multiple sensor platforms and capable of performing multiple-INTELLIGENCE (multi-INT) operations.² These Air Force units may best serve as examples for the remainder of this paper. In particular, one of these ground stations (DGS-2) has actively

participated in the U.S. and allied operations in the Balkans since the US's entry almost five years ago, including the recent NATO Operation ALLIED FORCE.³

BACKGROUND: DGS-2 AS AN ILLUSTRATION

Originally, DGS-2 was designed to support the U-2 reconnaissance aircraft in a deployed, stand-alone capacity. To do so, the ground station would sit within line-of-sight of the aircraft to perform near-real-time (NRT) exploitation of the information gathered by the aircraft's sensors.⁴ To perform its combat mission, the ground station would deploy along with some number of U-2 aircraft (in essence, a two part weapon system composed of the U-2 front end, and the DGS-2 back end). With the advent of modern communications technology, the ability emerged to locate the majority of the DGS-2 ground station outside of the aircraft's line-of-site by deploying only a single relay segment of the ground station within line-of-site.⁵ That small relay sends the digital information back to the rear-based ground station for exploitation. Additionally, DGS-2 retained the ability to operate the imagery sensors on board the aircraft in real time, loading and updating the collection plan, manually slewing the sensor as required, and providing the U-2 pilot direct steering queues to old targets requiring a second look, or to new targets added to the collection plan on an *ad hoc* basis. As a result, "dynamic retasking" remained an option, allowing one sensor set on the aircraft to detect an event with potential intelligence significance to either the tactical or operational commander, and then confirmation of that event with a second on board sensor.⁶ Once collection and exploitation of an intelligence event or target on the collection deck⁷ is complete, dissemination of the intelligence products is also accomplished virtually, with the combatant commander dictating a preferred format and dissemination method for the intelligence. Examples of the range of options available to the commander include voice reports, direct electronic delivery to a select electronic address (the ground station "pushes" the

information to the user) such as e-mail, posting images and data on a designated website (the user "pulls" the information when it is required), or any combination of these.

In effect, the same NRT support provided to the operational commander, when the ground station was located line-of-sight from the aircraft and in the combatant's theater, was maintained without the physical risk of placing an HD/LD, high-value intelligence asset close to the battlefield. Deployment costs were reduced. Personnel rotations were not required as with a traditional (physical) deployment to the theater. The list of benefits continues to grow today. Essentially, it is this capability that allowed DGS-2 to conduct operations other than war (OOTW) and wartime intelligence operations for EUCOM from its garrisoned location within the CONUS. The precedent is set, not only academically or theoretically, but also in practice for conducting virtual intelligence operations.

Since its inception, however, DGS-2 has broadened its capability in two distinct but related ways, courtesy of advances in computing and communications technology.⁸ It became the first ground station to operationally support two different geographic CINCs concurrently⁹, and it became a multi-platform ground station. DGS-2 conducted its first operational exploitation of Predator video for EUCOM during Operation ALLIED FORCE on 7 April 1999. This was in addition to and simultaneous with already established EUCOM U-2 missions. These are significant in and of themselves, but even more so when it is revealed that these demonstrated changes to the unit's depth and breadth of capability occurred without ever deploying.

During Operation ALLIED FORCE, DGS-2 performed multiple, synchronized U-2 and Predator missions, conducting intelligence operations independently for each system when required, and also queuing each sensor platform off the other when either required or prudent.¹⁰

Additionally, DGS-2 disseminated many correlated event reports (CERs) to the combat commander resulting from the correlation occurring between sensors onboard multiple, dissimilar platforms.¹¹ Although in its infancy, this models the picture that network-centric warfare advocates have painted for several years now. Multiple, dissimilar sensor platforms are feeding information into a grid (in this case, into the DGS) where all applicable pieces are assembled and exploited NRT to provide actionable intelligence products for the benefit the operational commander. These products are available to that commander through a mode and in the format of his choosing. Many of the CERs produced by DGS-2 were even disseminated as sensor-to-shooter packages, provided NRT to the cockpits of attack aircraft during strike operations.¹²

Today, DGS-2, and its sister DGS (DGS-1) are on the eve of adding additional sensors to their already robust network-based capability. Serving as the back end of both the U-2 and Predator reconnaissance systems, these units are scheduled to become the ground stations for Global Hawk, the Air Force's newest high altitude endurance (HAE) unmanned aerial vehicle (UAV), as well as for both commercial and national satellite imagery. It is important to note, however, that these are not isolated or "stovepipe" capabilities found within a single ground station. Although each sensor is platform-based, the ground station is network-based and therefore able to receive data from any one, some, or all of these sensors simultaneously, and if required, correlate or fuse the inputs into a single intelligence product or family of products NRT. Every class of intelligence product is available for dissemination to the operational commander through the avenue he selects. Additionally, this is done in a distributed fashion, allowing the DGS to share exploitation responsibilities with other units if required, and

intelligence product dissemination to single or multiple users at once, all from an in-garrison position.

During Operation ALLIED FORCE, DGS-2 processed U-2 derived imagery, and as a part of the exploitation, sent data through a virtual link to another geographically separated unit to derive precision coordinates for selected points on the image. DGS-2 would then fuse this information and provide it to the combat commander, all NRT. The picture here is of two CONUS-based units, geographically separated from each other, and from the command they operate with, providing NRT intelligence just as if they were physically located in the theater, and with the commander they serve.¹³

THE DILEMMA

Along with these benefits, however, come some reasonable concerns. As mentioned, DGS-2 has supported EUCOM from an in-garrison¹⁴ location from the time the unit gained operational status. The only concern this generated at the time revolved around the reliability of the link between the forward deployed relay segment in EUCOM and DGS-2 back in CONUS.

Network-based assets are relatively new for the U.S. military, and therefore the most efficient employment of their capability is still often misunderstood. Traditional weapons are platforms. This is true, it could be argued, from the simplest war club or battle axe of old, to the modern soldier, tank, ship or aircraft operating in today's battlespace. The capabilities of these assets are physical and therefore can only reside in one place at one time. As a result, if a traditional asset is deployed to operate in the EUCOM theater, it can not simultaneously operate in SOUTHCOM. A gain for one CINC equates to a loss for another—asset management being a zero-sum game. Because of this, the contemporary view of "ownership" (based on platforms) is

being understandably extended to emerging network-based assets. DGS-2, although a physical asset, deals exclusively in information. As the "techies" would say, it deals in "ones and zeros". Relative to the ground station, the locations of the physical sensors, the platforms that feed information into the network, are irrelevant, as are the numbers of sensors. One U-2 operating in a single theater is no more difficult than three in one theater and a UAV in another. Provided the network is up, the network-based asset (the DGS) functions.¹⁵ DGS-2's capability is virtual (not physical), therefore causing two significant changes to the fight. First, the physical DGS can be anywhere, and yet still provide the same quality and timely product to the combat commander. Second, since that product is virtual, it can go to any number of recipients simultaneously and with no loss in quality.

Sometimes current capabilities are also overrated when compared to the future capabilities described by network-centric warfare advocates. Networks today are not what they will most likely be in several years. If the technology experts are right, technology (to include bandwidth) are growing cheaper, and becoming more available at an exponential rate.¹⁶ Capabilities available today are robust, but they are not complete. Regardless, today's technology delivers a capability permitting a reasonable shift toward network-based capabilities and assets.¹⁷

To paraphrase a guest speaker's comments during a recent Joint Military Operations lecture at the Naval War College, "CINCs like to touch things. If they can't touch it, they don't feel like they own it." This is an understandable position driven by a history of platform-based weapons. Physical possession defines ownership. In the end, if the commander does not physically possess a thing, he is uncertain he can rely upon it. This creates the new dilemma as combat assets move from a platform basis to a network basis. This may best be illustrated by

looking at the marked success of DGS-2 and its performance of OOTW and combat intelligence operations across its existence.¹⁸ In spite of this success, including new capabilities demonstrated during Operation ALLIED FORCE, elements within U.S. European Command recently lobbied Headquarters, U.S. Air Force, to purchase a capability similar to the Army's Tactical Exploitation System¹⁹ so as to facilitate the comfort associated with "traditional ownership" of a platform-based asset. Although there is merit to maintaining some capability within the theater, the potential exists to relegate the more capable network-based system to taskings that are less time critical simply because it does not physically sit in the theater.²⁰

Generally speaking, if the network (something unseen) is reliable, it makes no difference if your ground station is in the building next door or in the next country. To further feed and complicate this concern, however, I refer back to my earlier statement about the nature of the example above: the U-2/DGS-2 weapon system. Viewing the U-2 as the sensor and as only one half of a weapon system, asking a CINC to trust that success will flow from possessing only half of a weapon, while the other half sits in some far away place well removed from the battlefield and theater only serves to cause some measure of stress. This stress grows when this same CINC is told he may share this network-based asset with another CINC. The concern and stress is understandable. Even more so when this stress runs in concert with the risk of combat operations. Tradition has engrained the combat commander with the knowledge that if he does not possess the asset, at best he will most likely lose it, and worse yet, it will not perform for him at all. Nonetheless, recent history, best demonstrated during Operation ALLIED FORCE, was the first giant step in credibly putting these concerns to rest. The demonstration made clear the time has come to embrace networked capabilities and a network-based doctrine for the employment of network-based military assets. The new model of ownership no longer always

obligates physical assets to a CINC. Instead, along with certain platforms, the CINC will have "ownership" of network-based information.

A CHANGE IN CULTURE

Due to the technological nature of today's military, I believe that most members of the armed forces under the age of 35 (and many over that age) have a strong knowledge of the popular network known as the Internet or World Wide Web. Most of these with strong knowledge probably have as much faith in that networks reliability and survivability as they do in the electricity that powers it. It is inconceivable to most of this group that the Internet at large will fail, in spite of the periodic failure of numbers of nodes it contains. Reliability is the beauty of a network. Reliability and survivability were the very reasons the Department of Defense facilitated the creation of what became the Internet (in its original form, linking several universities).²¹ It has since grown into "a network of networks that spans the globe."²² Although the Internet has moved primarily into the civil domain, the capabilities it parented still remain within the DoD. Nonetheless, most senior leaders within the department still hesitate to embrace these capabilities unless they are employed as platforms, dampening, if not quenching the broader and deeper capabilities afforded by the network. It seems a steady cultural shift is called for, moving the Department of Defense methodically from a platform-based mindset to one that is network-based. Without abandoning the capabilities that platforms bring to the table, the new focus must be on capabilities that are orders of magnitude beyond those afforded by platforms alone.

MOVING BEYOND THE CONCEPTUAL TEMPLATE

Joint doctrine is perhaps the best vehicle to begin to address this issue in a manner that meets today's requirements, and keeps a framework/establishes a foundation flexible enough to

incorporate the emerging and increased use of network-based assets (the movement toward network-centric warfare). As mentioned, JV 2010 has already established the foundation upon which doctrine for network-based assets can be built. The introduction states that "Joint Vision 2010 is the conceptual template for how America's Armed Forces will channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting."²³ Later in the document, this statement is followed by:

Improvements in information and systems integration technologies will also significantly impact future operations by providing decision makers with accurate information in a timely manner. Information technology will improve the ability to see, prioritize, assign, and assess information. The fusion of all-source intelligence with the fluid integration of sensors, platforms, command organizations, and logistic support centers will allow a greater number of operational tasks to be accomplished faster. *Advances in computer processing, precise global positioning, and telecommunications will provide the capability to determine accurate locations of friendly and enemy forces, as well as to collect, process, and distribute relevant data to thousands of locations*" (emphasis mine)²⁴.

Units like the Air Forces DGS-2, tied to the Distributed Common Ground System (DCGS)²⁵, are beginning to deliver this very capability. Joint doctrine must now move from the conceptual framework to the specifics of employing these assets. Available technology and associated circumstance have delivered the opportunity to move forward. Within the context of Full-Dimensional Protection, JV2010 continues, "Passive measures will include the inherent protection provided by information superiority and dispersal to increase our warning of attacks. *Operational dispersion will further reduce risks to our forces.*" (emphasis mine).²⁶ These statements made in the future tense are now in practice today on a small scale. At this point, the circumstances and technology have brought us full-circle.

A RELATED ISSUE: "DEPLOYED IN-GARRISON"

New doctrine and related Service policies for employing network-based assets must fall in behind the Joint Vision template in both form and function. This will also mandate some related changes in traditional views about and definitions of concepts such as what constitutes deployment to and participation in an operation or campaign. Generally the question is "how far is too far from the battlefield?" Long ago, if you did not engage the enemy face to face, you were not a participant. With the advent of "long range weapons", what defined the boundary for participation grew. Artillery crews who fired rounds well outside of their line of sight but may have never seen an enemy soldier, or aircrews who flew into the battle area from bases not directly in harms' way were considered combatants. Today, it is less than common, but not uncommon for aircrews to depart their home base in CONUS to execute combat sorties almost half a world away. Units that deal in information, the network-based assets mentioned above also fall into this category. These assets and weapon systems are further removed from the battlespace than the generation before. Nonetheless, their participation is no less than their predecessors who had to physically locate in the area of operation, a neighboring country, or somewhere else in the theater. Today, "standoff" and "reachback" allow combat basing even in the CONUS for some assets. Deployment and participation in OOTW and wartime operations must be redefined to accommodate these emerging virtual and long-range assets. Just as no one would suggest that an aircraft flown off of an aircraft carrier or base in a country located well outside of direct combat is not a true participant in the fight simply because of its point of origin, the same logic should apply to network-based assets.

There are those who would imply or suggest, however, that participation is somehow tied to a literal deployment to and residence in the theater. A contemporary example of this is the

debate revolving around the Kosovo Campaign Medal. While there are senior service leaders advocating awarding this medal to all participants, including those who operated from a “reachback” or distributed position, there are other senior leaders who are in opposition, advocating that these units and individuals (primarily aircrews and intelligence professionals) do not merit the award or credit for participation in the sense that those do that physically deployed to the theater and then operated (even if still in a reachback configuration—just with less distance between the ends). What this does demonstrate is the clash between the traditional and new models of ownership on a very practical level. It also illustrates the level of detail the new doctrine must extend to.

POSSIBLE SOLUTIONS

To begin a deliberate movement from a military culture oriented to the platform-based weapon system, toward one that recognizes the role platforms play in a network-based military, four options illustrate general concepts for bringing doctrine beyond the starting point afforded in JV 2010. These options are intended to suggest ways to organize so as to best bring the benefits of contemporary network-based assets to the table without degrading (and in fact, dramatically improving) current and future warfighting capabilities.

The first suggestion essentially acknowledges where we are today, but remains a valid way to task and use network-based assets. The Department of Defense can treat network-based assets as platforms. Essentially, this is a “first come, first serve” arrangement, where assets are apportioned to multiple CINCs for planning purposes, but are only be available to one, based on circumstance. Network-based assets will be tasked to support the single combat commander who has the highest priority tasking relative to what that asset can contribute. Those coming later must negotiate with the current “owner” for the asset or even reclama to the Joint Staff for a

change of ownership. This is not to suggest that the network-based asset could not perform in a manner that exploits the benefits of the network from a deployed location. Rather, the problem may arise when a CINC fears losing some capability (real or imagined) by sharing the asset.

Second is what can be called "third party ownership". This is to say that the network-based asset is permanently "owned" by a CINC who will most likely always be designated in a supporting role. For example, organizations such as the DGSs could permanently fall under U.S. Joint Forces Command (USJFCOM) as the acknowledged "force provider" for the other CINCs. A second option would be to assign them to U.S. Space Command; a Command with no ties to any geographic region. These CINCs could then serve as "honest brokers" and could balance asset capabilities with multiple requests and taskings. Additionally, if an asset approaches the limits of its capabilities (perhaps due to manning levels), the supporting CINC becomes the responsible party for adjudicating competing requests.

Third, designate network-based assets (especially HD/LD) as "national assets", similar to many platform-based assets today. These limited assets would then be requested, tasked and managed just as current national assets are.

Finally, the formation of a new unified command, perhaps called U.S. Information Command (USINFOCOM), may be warranted sometime in the not too distant future. This command, functional in nature, would hold responsibility similar to other existing unified commands, tasked to manage and employ all network-based assets. It would almost always be designated as a supporting command to a geographic CINC, and would serve as the honest broker between the potentially competing interest of other CINCs. This command could be modeled after similar commands that exist today, such as USSOCOM, USSTRATCOM, USTRANSCOM or USSPACECOM.

RECOMMENDATIONS

Following are four recommendations that will help facilitate the DoD migration from being fully platform focused, to a focus that embraces not only platforms, but network-based weapon systems as well. First, Joint doctrine must move beyond the conceptual framework established by JV 2010. As systems like DGS-2, and the Air Force's DCGS emerge, Joint and Service doctrine must acknowledge these assets for what they are (networks, not platforms), and address the tactics, techniques and procedures for their tasking and employment that best bring their capabilities to bare across the range of military operations.

Second, what can only be called "marketing" is required. This in essence means that the Services must highlight these assets as unique, and call proper attention to the new capabilities they bring to operational and tactical commanders. The current series of Joint Publications, as well as JV 2010 serve as examples. These high-quality documents look good and read well. Something similar is called for with the advent of these network-based assets, drawing needed attention to the capability. These documents must, however, go beyond JV 2010 in that the level of detail required is greater. Services that develop these network-based assets, and provide them to the warfighter, must not only say that they have some new (and different) tool they can bring to the fight, but also explain how the tool is different in form and function. Additionally, the Services must express how to best task for and use the asset.

The "marketing" then leads to the third recommendation: education and training. Since the publication of JV 2010, knowledge of what the document represents has grown over time. The same must occur as emphasis is placed on network-based assets. Within the Services, the elements that own these assets must educate those who desire to task them. At the Unified Command level, using DGS-2 as the example, the Numbered Air Force it falls under must ensure

that the ground station is made available for training and exercises, and that its true capability and function is properly understood by those making the request. Exercises may be the best vehicle for this. DGS-2 has participated in numerous Service (Air Force, Marine Corps and Navy) exercises, as well as joint exercises and experiments. Due to operational commitments to USEUCOM, DGS-2 was obligated to continue performing from an in-garrison position, providing virtual support to the event, and by default, educating and training future operational users as to the capabilities the asset can bring to the fight.

Fourth and finally, for the immediate future, and for intelligence related assets specifically, placing these HD/LD assets under a unified commander who will generally always be assigned in a supporting role relative to a geographic CINC seems prudent. Units such as the Air Force's DGSs, and its DCGS network will probably best serve the CINCs if they are "owned" by either US Joint Forces Command or US Space Command. These combatant commands can serve as the honest brokers to best showcase the capabilities and limitations of these assets in the joint world, and could do so across the range of military operations.

CONCLUSION

The Air Force's Distributed Common Ground System, and the DGS-2 interface with this network are not the complete solution, nor are they examples of all that is required to bring the military from an industry base to an information base. The Air Force, however, has moved from an academic and theoretical acceptance of the concept of network-based weapons, to implementing a rudimentary network. Beyond this, they have employed it, primarily due to circumstances revolving around funds and force protection issues, but employed it nonetheless. What was once only discussed has now been put into practice. Building upon the conceptual framework analogy expressed in JV 2010, the Air Force has hung one of the first walls on the

future structure we often hear described as “network-centric warfare”. The other Services are certainly working in the same direction. Representatives from the services and industry met last year in San Diego, California at the first Intelligence, Surveillance and Reconnaissance Systems Conference. At this assembly, representatives from each of the Service Staffs briefed their perspectives and progress made on their Service’s DCGS programs. To this, add new DoD standards established to ensure future systems are interoperable²⁷, and it appears as a military, we are on our way toward developing credible network-based capabilities within the ISR community, and eventually across the DoD in all functional areas. At this point, what is left is to move our military culture in a new direction, embracing network-based capabilities and assets, while maintaining a balanced appreciation for what the associated platforms continue to bring to the fight.

NOTES

¹ John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: RAND, 1997), 5-6.

² "Multi-INT operations" refers to the use of data from two or more synergistic intelligence disciplines, including the compilation of correlated data and generation of correlated intelligence products. Reference: Operational Requirements Document (ORD) CAF 304-96-I for Distributed Common Ground Systems (DCGS), 1 October 1999.

³ DGS-2 declared Initial Operating Capability on or about 10 July 1995 and was subsequently tasked to perform intelligence operations from an in-garrison position for USEUCOM on 6 November 1995. The unit has maintained continuous operations supporting EUCOM since that day without deploying to the theater. Between the IOC declaration and receipt of the OPORD, significant discussion occurred over whether or not to deploy the entire ground station, or to deploy a relay segment forward and leave the ground station in-garrison. Ultimately, the decision was made to perform reachback operations to defray costs. (Circumstantially driven.) "In-garrison" is defined below, in endnote 14.

⁴ Throughout this paper, references to NRT imagery exploitation refers to digital imagery. The U-2 also maintains the capability to carry a traditional "wet film" sensor, however, exploitation of wet film can not occur in near real time as the film can only be removed from the aircraft after landing. Additional delay then results due to time required for development of the film. Post development, these images can be digitized, however the delay caused by this total process exceeds what can be considered NRT. Digital images composed the preponderance of those taken over the Balkans (including during Operation ALLIED FORCE).

⁵ This segment of the DGS-2 compound, and the associated architecture it facilitates is called Mobile Stretch (or "MOBSTR").

⁶ These singular intelligence events collected by multiple sensors on the U-2 are commonly referred to as "Correlated Event Reports", or CERs.

⁷ "Collection Deck" is a term used to describe the order in which a predetermined set of targets will be collected against on a particular sensor mission. It is not uncommon to adjust the deck, as mission needs dictate, either to accomplish a second look at a previous target or to add an additional (ad hoc) target not originally included in the deck.

⁸ The Air Force recently changed the acronym "DGS" to mean "Distributed Ground System". There are currently four DGSs, one of which is not deployable. DGS-2 remains a deployable asset but also serves with the other DGSs as a core location on the emerging DCGS Processing, Exploitation and Dissemination Architecture. This network is designed to provide near real-time, fused intelligence products to the warfighter. It is comprised of the geographically separated DGS elements, linked electronically (networked) to create the DCGS. Reference: DCGS ORD, 1 October 1999.

⁹ While operating for EUCOM as a U-2 ground station, DGS-2 was tasked to provide concurrent U-2 ground station operations for USSOUTHCOM in February 1998. More recently, when EUCOM's Predator operations terminated during Operation JOINT GUARDIAN, and the airframes redeployed to their CONUS base, DGS-2 deployed its UAV Exploitation System (a DGS-2 component) within the CONUS as a participant in GLOBAL GUARDIAN, serving as the Global Hawk groundstation. U-2 intelligence operations continued uninterrupted for EUCOM while DGS-2 simultaneously conducted intelligence operations for USSTRATCOM. This further demonstrates the flexibility afforded to multiple combatant commanders through the proper use of these flexible, modular and scalable network-based assets.

¹⁰ There are significant doctrinal issues needing to be addressed regarding sensor control or "sensor ownership" for the Predator. Currently, the aircrews who operate the airframe from a forward-deployed location also control the sensor. The level of coordination required between the DGS mission crew and the aircraft mission crew to pass requests from the intelligence unit to the individual physically controlling the sensor is cumbersome. The Air Force may best serve the combatant commander if Predator sensor control resides with the intelligence unit, as is the current practice with the U-2. The U-2 mission planning and collection planning marriage, and sensor operation procedures are a model of success. Mission success rates for dynamic sensor control and retaskings are available through Air Combat Command, ACC/XOIRY.

¹¹ DGS-2 issues a total of 103 CERs during Operation ALLIED FORCE, many of which were based on multi-platform correlation.

¹² DGS-2 disseminated 66 total sensor-to-shooter packages during ALLIED FORCE, most based on CERs.

¹³ Other virtual links to units geographically separated from the combatant commander and DGS-2 existed, and were used to facilitate creating NRT intelligence products for EUCOM. These links are not addressed in this paper due to classification.

¹⁴ For the purposes of this paper, "in-garrison" is defined as the normal peacetime location where a military unit, untasked to support an exercise or operation, is found. DGS-2's in-garrison location is Beale AFB, California.

¹⁵ This is not to suggest that there are not limitations imposed on networks or network-based assets by issues such as manpower, logistics, sustainment, etc. The purpose here is not to address manning issues. Rather, proper manning, logistics, sustainment, etc. is assumed here in order to help clarify differences between platform and network-based capabilities. Although network-based assets may relieve some strains caused by these traditional problems, they do not eliminate them.

¹⁶ According to Larry Downes and Chunka Mui, "computing power and communications bandwidth, thanks to Moore's Law, are becoming cheap enough to treat as disposable." (Moore's Law essentially states that "every eighteen months, processing power doubles while cost holds constant.") Larry Downes and Chunka Mui, *Unleashing the Killer App: Digital Strategies for Market Dominance* (Boston: Harvard Business School Press, 1998), 21, 65.

¹⁷ The network supporting DGS-2 (and other nodes) is significant when measured by the bandwidth available across the network. Specific data regarding network maintenance and control is classified.

¹⁸ Specific mission success rates and reasons for mission aborts are classified, however, the DGS-2 success rate falls above 95%.

¹⁹ The Tactical Exploitation System (TES) is a multi-INT exploitation asset designed to operate at the tactical level. A U.S. Army fact sheet is available on the World Wide Web at: <http://www.smdc.army.mil/FactSheets/TES.html>. While quite capable, TES is designed to obligate the location of workstations (platforms) forward (along with associated crews), albeit in minimal numbers. The forward element of TES is mounted on the military HMMWV allowing for mobility. Although this system is scalable, its platform orientation mandates limits to workstations and continues to place high-value assets at risk. The DGS is also deployable, modular, and scalable, but does not obligate forward deploying analysts and workstations. Intelligence is provided (as with TES), but through a robust network (DCGS) and either pushed to or pulled by the combat commander based on his requirements.

²⁰ Across DGS-2's operations in support of USEUCOM, intelligence products' formats and method of delivery have been dictated by the theater. To date, DGS-2 has provided these products in a manner consistent with the theater's requirements. This continued through Operation ALLIED FORCE, when special web sites were created on SIPRNET and JWICS to facilitate theater requirements for posting new products. This occurred in addition to the pushing and pulling of other, already established products.

²¹ Larry Downes and Chunka Mui, *Unleashing the Killer App: Digital Strategies for Market Dominance* (Boston: Harvard Business School Press, 1998), 6.

²² Dorothy E. Denning, *Information Warfare and Security* [Reading: ACM Press, 1999], 14.

²³ Joint Chiefs of Staff, *Joint Vision 2010*, Washington, D.C., n.d., 1.

²⁴ *Ibid.*, p. 13.

²⁵ The DCGS Operations Requirements Document defines DCGS as "a multi-intelligence, common, interoperable, open ground system architecture." It then continues, "Accordingly, each Service will develop a unique implementation of this architecture that best supports their war-fighting concepts and doctrine... The Air Force DCGS... distributes multi-INT TPED [tasking, processing, exploitation and dissemination] functionality and responsibility across AF intelligence organizations to take advantage of data collected by national, theater, commercial and tactical ISR collection sensors. It effectively eliminates the concept of stove-piped, proprietary platform-based TPED ground stations and organizations. As an architecture, the DCGS is a "system of systems" that connects geographically separated fixed and deployable ISR ground stations via a wide area network to create a virtual multi-INT TPED environment. The system will simultaneously task and receive, process, exploit and disseminate data from national, theater, tactical and commercial collection assets in a distributed environment. It will support national, joint, combined, an AF operations. It will be capable of forward deployed, split-based, and in-garrison Reachback operations, and will leverage the capabilities of fielded and planned ISR TPED systems."

²⁶ Joint Chiefs of Staff, *Joint Vision 2010*, Washington, D.C., n.d., 23.

²⁷ These standards define common information formats. For example, they cover data such as various the various forms of digital imagery. DoD has not defined how each Service will build or develop the hardware associated with these imagery formats. Rather, it dictates the format that digital imagery must be sent and received by any system developed for use by a Service. The end result is a basic level of interoperability.

BIBLIOGRAPHY

- Adams, James. *The Next World War: Computers Are the Weapons and the Front Line is Everywhere*. New York: Simon and Schuster, 1998.
- Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority Second Edition (Revised)*. Washington D.C.: CCRP, 1999.
- Arquilla, John. "The 'Velvet' Revolution in Military Affairs." *World Policy* (Winter 1997/1998): 32-43.
- Arquilla, John and David Ronfeldt. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND, 1997.
- Barsaleau, Dean. "CEC: The Unprecedented Force Multiplier." *Surface Warfare* (September/October 1994): 22-27.
- Bower, Joseph L. and Clayton M. Christensen. "Disruptive Technologies: Catching the Wave." *Harvard Business Review* (January-February 1995): 43-53.
- Buhl, Lance C. "Mariners and Machines: Resistance to Technological Change in the American Navy, 1865-1869." *The Journal of American History* 61, no. 3 (December 1974): 703-727.
- Bunker, Robert J. "The Transition To Fourth Epoch War." *Marine Corps Gazette* 78, no. 9 (September 1994): 20-30.
- Cebrowski, Arthur K. "Network-Centric Warfare—Its Origin and Future." *Proceedings* 124, no. 1/1, 139: 28-35.
- Clausewitz, Carl von. *On War*. Translated and edited by Michael Howard and Peter Paret. New Jersey: Princeton University Press, 1976.
- Cohen, Eliot A. "A Revolution in Warfare." *Foreign Affairs* 75, no. 2 (March/April 1996): 37-54.
- Crevelld, Martin van. *The Transformation of War*. New York: The Free Press, 1991.
- Denning, Dorothy E. *Information Warfare and Security*. Massachusetts: Addison-Wesley, 1999.
- FitzSimonds, James R. "The Cultural Challenge of Information Technology." *Naval War College Review* 50, no. 3 (Summer 1998): 9-21.
- _____. "Intelligence and the Revolution in Military Affairs." In *U.S. Intelligence at*

the Crossroads, ed. Roy Godson, Ernest R. May, and Gary Schmitt, 265-287. Brassey's, 1995.

Goldman, Emily O. "The U.S. Military in Uncertain Times: Organizations, Ambiguity, and Strategic Adjustment." *The Journal of Strategic Studies* 20, no. 2 (June 1997): 41-74.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. *Information Warfare and International Law*. Washington, D.C.: National Defense University, 1997.

Krepinevich, Andrew F. "Cavalry to Computer: The Pattern of Military Revolutions." *The National Interest* (Fall 1994): 30-42.

Murray, Williamson. "Thinking About Revolutions in Military Affairs." *Joint Force Quarterly* (Summer 1997): 69-76.

Peters, Ralph. "After the Revolution." *Parameters: U.S. Army War College Quarterly* 25, no. 2 (Summer 1995), 7-14.

Schnaubelt, Christopher M. "Lessons in Command and Control from the Los Angeles Riots." *Parameters: U.S. Army War College Quarterly* 27, no. 2 (Summer 1997), 88-109.

Schwartz, Winn. *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Information Age*. New York: Thunder's Mouth Press, 1996.

Toffler, Alvin and Heidi. *War and Antiwar: Making Sense of Today's Global Chaos*. New York: Warner Books, Inc., 1993.

Zorpette, Glenn. "A New Fat Pipe." *Scientific American*, April 1998, p. 34.

U.S. GOVERNMENT DOCUMENTS

U.S. Department of the Air Force. *Operational Requirements Document CAF 304-96-I For Distributed Common Ground System (DCGS) (U)*. Washington, D.C.: 1 October 1999.

U.S. Department of Defense. *Annual Report to the President and Congress 1999*, pp. 121-137, 139-146.

U.S. Department of the Navy. *The Commander's Handbook on the Law of Naval Operations* (NWP 1-14M) Newport: October 1995.

U.S. Joint Chiefs of Staff. *Joint Vision 2010*. Washington, D.C.: n.d.

OTHER SOURCES

Godfrey, Sean <Sean.Godfrey@beale.af.mil> "RE: RE: HOT—DGS-2 Info." 7 February 2000. Personal e-mail. (7 February 2000).

Grundhauser, Larry K. <larry.grundhauser@beale.af.mil> "RE: DGS Tasking in the Future." 20 January 2000. Personal e-mail. (20 January 2000).

Malm, Rollen <Rollen.malm@beale.af.mil> "RE: RE: HOT—DGS-2 Info." 3 February 2000. Personal e-mail. (3 February 2000).

Stoney, Anthony E. <Anthony.Stoney@langley.af.mil> "RE: HOT--Distributed Ops Info." 31 January 2000. Personal e-mail. (31 January 2000).

West, Kevin <Kevin.West@pentagon.af.mil> "RE: DGS Tasking in the Future." 10 January 2000. Personal e-mail. (10 January 2000).